

METHOD FOR CLIENT DELEGATION OF
SECURITY TO A PROXY

ABSTRACT OF THE DISCLOSURE

5 A method of enabling a proxy to participate in a
secure communication between a client and a server. The
method begins by establishing a first secure session
between the client and the proxy. Upon verifying the
first secure session, the method continues by
10 establishing a second secure session between the client
and the proxy. In the second secure session, the client
requests the proxy to act as a conduit to the server.
Thereafter, the client and the server negotiate a session
master secret. Using the first secure session, this
15 session master secret is then provided by the client to
the proxy to enable the proxy to participate in secure
communications between the client and the server. After
receiving the session master secret, the proxy generates
cryptographic information that enables it to provide a
20 given service (e.g., transcoding, monitoring,
encryption/decryption, caching, or the like) on the
client's behalf and without the server's knowledge or
participation. The first secure session is maintained
between the client and the proxy during such
25 communications.

006372.00209:0424649.01